Claims

1. A system for automatically handling Internet Key Exchange (IKE) traffic in a virtual private network (VPN), comprising:

a filter detection system for searching for IKE traffic permit filters;

an IKE traffic enablement system for automatically allowing IKE traffic to flow if the IKE traffic permit filters are not detected; and

an IKE traffic management system for managing the IKE traffic through VPN connections.

2. The system of claim 1, wherein the filter detection system searches for IKE traffic permit filters on a first node.

3. The system of claim 2, wherein the IKE traffic enablement system automatically allows IKE traffic to flow between the first node and a second node if IKE traffic permit filters are not detected by the filter detection system.

4. The system of claim 3, wherein the IKE traffic that flows between the first node and the second node establishes security associations for a VPN connection between the first node and the second node.

5. The system of claim 4, wherein the IKE traffic enablement system automatically allows refreshing IKE traffic to flow between the first node and the second node, and wherein the refreshing IKE traffic is guided outside of the VPN connection by the IKE traffic management system.

6. The system of claim 5, wherein the refreshing IKE traffic is secured by the first node and the second node.

7. The system of claim 1, wherein the IKE traffic management system references a table containing entries that identify connections between nodes, IP addresses of connected nodes, and security associations for the VPN connections.

8. The system of claim 7, wherein the IKE traffic management system guides IKE traffic pertaining to a nested VPN connection outside of the nested VPN connection in a secured mode based upon the security associations between the first node and the second node identified in the table.

9. A system for automatically handling Internet Key Exchange (IKE) traffic in a virtual private network (VPN), comprising:

a filter detection system for searching for IKE traffic permit filters on a first node;

an IKE traffic enablement system for automatically allowing IKE traffic to flow between the first node and a second node if the IKE traffic permit filters are not detected; and

an IKE traffic management system for managing outbound IKE traffic from the first node to the second node, wherein the outbound IKE traffic is guided outside of a VPN connection between the first node and the second node.

10. The system of claim 9, wherein the IKE traffic between the first node and the second node establishes security associations for an outer VPN connection.

11. The system of claim 9, wherein the IKE traffic enablement system further automatically allows IKE traffic to flow between the first node and a remote node to establish security associations for a nested VPN connection between the first node and the remote node.

12. The system of claim 11, wherein refresh IKE traffic between the first node and the remote node flows outside of the nested VPN connection.

13. The system of claim 9, wherein the IKE traffic management system references a table to determine a proper connection through which the outbound IKE traffic from the first gateway node should be guided, and wherein the table contains entries that identify VPN connections between nodes, IP address of connected nodes, and security associations for the VPN connections.

14. A method for automatically handling Internet Key Exchange (IKE) traffic in a virtual private network (VPN), comprising the steps of:

searching for IKE traffic permit filters on a first node;

automatically allowing IKE traffic to flow in and out of the first node if the IKE traffic permit filters are not detected; and

managing outbound IKE traffic from the first node, wherein the outbound IKE traffic is guided outside of a particular VPN connection to which it pertains.

15. The method of claim 14, wherein managing step comprises the steps of:

accessing a table to identify the particular VPN connection to which the outbound IKE traffic pertains; and

routing the IKE traffic outside of the identified VPN connection.

16. The method of claim 15, further comprising the step of securing the IKE traffic flowing in and out of the first node.

17. A method for automatically handling Internet Key Exchange (IKE) traffic in a virtual private network (VPN), comprising the steps of:

searching for IKE traffic permit filters on a first node;

automatically allowing IKE traffic to flow between the first node and a second node if the IKE traffic permit filters are not detected; and

establishing security associations between the first node and the second node for an outer VPN connection.

18. The method of claim 17, further comprising the step of managing outbound IKE traffic from the first node, wherein the outbound IKE traffic pertaining to the outer VPN connection is guided outside of the outer VPN connection, and wherein the outbound IKE traffic pertaining to a nested VPN connection between the first node and a remote node is guided outside of the nested VPN connection.

19. The method of claim 18, wherein the managing step comprises the steps of:

referencing a table that identifies VPN connections between nodes, IP addresses of connected nodes, and security associations for the VPN connections;

routing the outbound IKE traffic pertaining to the outer VPN connection outside of the outer VPN connection; and

routing the outbound IKE traffic pertaining to the nested VPN connection outside of the nested VPN connection.

20. A method for automatically handling Internet Key Exchange (IKE) traffic in a virtual private network (VPN), comprising the steps of:

searching for IKE traffic permit filters on a first node;

automatically allowing IKE traffic to flow between the first node and a second node if the IKE traffic permit filters are not detected;

establishing security associations between the first node and the second node for an outer VPN connection;

automatically allowing IKE traffic to flow between the first node and a remote node;

establishing security associations between the first node and the remote node for a nested VPN connection within the outer VPN connection; and

managing outbound IKE traffic from the first node, wherein the outbound IKE traffic pertaining to the outer VPN connection is guided outside of the outer VPN connection, and wherein the outbound IKE traffic pertaining to the nested VPN connection is guided outside of the nested VPN connection.

21. The method of claim 20, further comprising the step of securing the IKE traffic between the first node and the remote node based upon the security associations established between the first node and the second node.

22. The method of claim 20, wherein the managing step comprises the steps of:

referencing a table that identifies VPN connections, IP addresses of connected nodes, and security associations for the VPN connections;

routing the outbound IKE traffic from the first node to the second node outside of the outer VPN connection; and

routing the outbound IKE traffic from the first node to the remote node outside of the nested VPN connection in a secured mode based upon the security associations between the first node and the second node identified in the table.

23. The method of claim 20, further comprising the steps of:

receiving an inbound IKE communication in the first node from the remote node through the outer VPN connection;

creating a potential nested VPN connection entry in a table, wherein the entry identifies a potential nested VPN connection and IP addresses corresponding to the remote node and the first node;

negotiating security associations between the remote node and the first node;

loading the nested VPN connection between the remote node and the first node; and

updating the table by replacing the potential VPN connection with the nested VPN connection.

24. A program product stored on a recordable medium for automatically handling Internet Key Exchange (IKE) traffic in a virtual private network (VPN), which when executed, comprises:

program code configured to search for IKE traffic permit filters;

program code configured to automatically allow IKE traffic to flow if the IKE traffic permit filters are not detected; and

program code configured to manage the IKE traffic through VPN connections.

25. The program product of claim 24, wherein the IKE traffic permit filters are searched for on a first node.

26. The program product of claim 25, wherein the IKE traffic is automatically allowed to flow between the first node and a second node if IKE traffic permit filters are not detected.

27. The program product of claim 26, wherein the IKE traffic that flows between the first node and the second node establishes security associations for a VPN connection between the first node and the second node.

28. The program product of claim 27, wherein IKE refreshing traffic is automatically allowed to flow between the first node and the second node outside of the VPN connection.

29. The program product of claim 28, wherein the refreshing IKE traffic is secured by the first node and the second node.

30. The program product of claim 24, wherein the IKE traffic for VPN connections is managed based upon a table containing entries that identify connections between nodes, IP addresses of connected nodes, and security associations for the VPN connections.

31. The program product of claim 30, wherein the IKE traffic pertaining to a nested VPN connection is guided outside of the nested VPN connection in a secured mode based upon the security associations between the first node and the second node identified in the table.